

# Suslin's lemma for elimination

Ihsen Yengui (<sup>1</sup>)

April 25, 2007

## Abstract

The purpose of this paper is to study algorithmically an important lemma of Suslin which turned out to be useful for eliminating variables and decisive in Suslin's second solution of Serre's conjecture, that is, in his elementary proof that finitely generated projective modules over  $\mathbf{K}[X_1, \dots, X_n]$ ,  $\mathbf{K}$  a principal domain, are free. This lemma says that for a commutative ring  $\mathbf{A}$ , if  $\langle v_1(X), \dots, v_n(X) \rangle = \mathbf{A}[X]$  where  $v_1$  is monic and  $n \geq 3$ , then there exist  $\gamma_1, \dots, \gamma_\ell \in E_{n-1}(\mathbf{A}[X])$  such that  $\langle \text{Res}(v_1, e_1 \cdot \gamma_1^t(v_2, \dots, v_n)), \dots, \text{Res}(v_1, e_1 \cdot \gamma_\ell^t(v_2, \dots, v_n)) \rangle = \mathbf{A}$ .

In fact, this lemma is the only nonconstructive step in Suslin's elementary proof of Serre's conjecture. The problem with Suslin's proof is that it does not give an explicit way to find the elementary operations  $\gamma_i$  since it reasons modulo each maximal ideal of  $\mathbf{A}$ . Of course this is important for concrete applications in circuits, systems controls, signal processing, and other areas. We will give an algorithm realizing Suslin's lemma for any ring  $\mathbf{A}$ . A detailed example of a unimodular completion of a vector in  $\text{Um}_3(\mathbb{Z}[X])$  will be given.

In the particular case where the basic ring  $\mathbf{A}$  contains an infinite field, we give a more precise and simpler version of this lemma. As a matter of fact, using a new definition of the resultant, we will give a simplified formulation of Suslin's lemma. As application to our study of Suslin's lemma, we give two simple algorithms for unimodular completion (the Quillen-Suslin theorem). The first one is over rings  $\mathbf{A}$  containing an infinite field. This algorithm has been implemented with the computer algebra system Maple. The second one is over any ring  $\mathbf{A}$  and is partially implemented.

MSC 2000 : 13C10, 19A13, 14Q20, 03F65.

Key words : Suslin's lemma, Quillen-Suslin theorem, resultant, radical of an ideal, commutative algebra, algebraic geometry, constructive mathematics, computer algebra.

## 1 Suslin's lemma, general case

Our first motivation in this paragraph is to find an algorithm establishing a lemma of Suslin [16] (Lemma 2.3) which played a central role in Suslin's second solution of Serre's conjecture, that is, in his elementary proof that finitely generated projective modules over  $\mathbf{K}[X_1, \dots, X_n]$ ,  $\mathbf{K}$  a principal domain, are free. This lemma says that for a commutative ring  $\mathbf{A}$ , if  $\langle v_1(X), \dots, v_n(X) \rangle = \mathbf{A}[X]$  where  $v_1$  is monic and  $n \geq 3$ , then there exist finitely many  $\gamma_i \in E_{n-1}(\mathbf{A}[X])$ , the subgroup of  $\text{SL}_{n-1}(\mathbf{A}[X])$  generated by elementary matrices, such that  $\langle \text{Res}(v_1, e_1 \cdot \gamma_i^t(v_2, \dots, v_n)), 1 \leq i \leq \ell \rangle = \mathbf{A}$ .

In fact, the lemma cited above is the only nonconstructive step in Suslin's elementary proof of Serre's conjecture [16]. The problem with Suslin's proof is that it does not give an explicit way to find the elementary operations  $\gamma_i$  since it reasons modulo each maximal ideal of  $\mathbf{A}$  (see [18] for a general strategy for rereading constructively such proofs). Of course this is important for concrete applications in circuits, systems controls [5, 6, 19], signal processing [12, 13], and other areas [8, 9].

Recall that for any ring  $\mathbf{B}$  and  $n \geq 1$ , an  $n \times n$  elementary matrix  $E_{i,j}(a)$  over  $\mathbf{B}$ , where  $i \neq j$  and  $a \in \mathbf{B}$ , is the matrix with 1s on the diagonal,  $a$  on position  $(i, j)$  and 0s elsewhere, that is,  $E_{i,j}(a)$  is

---

<sup>1</sup> Departement of Mathematics, Faculty of Sciences of Sfax, 3038 Sfax, TUNISIA, email: ihsen.yengui@fss.rnu.tn.

the matrix corresponding to the elementary operation  $L_i \rightarrow L_i + aL_j$ .  $E_n(\mathbf{B})$  will denote the subgroup of  $SL_n(\mathbf{B})$  generated by elementary matrices.

Recall also that  $Um_n(\mathbf{B}) := \{ {}^t(x_1, \dots, x_n) \in \mathbf{B}^n \text{ such that } \langle x_1, \dots, x_n \rangle = \mathbf{B} \}$  is called the set of unimodular vectors with  $n$  entries in  $\mathbf{B}$ .

As usual, if  $P$  is a subset of  $\mathbf{B}$ , we will denote by  $\langle P \rangle$  the ideal of  $\mathbf{B}$  generated by the elements of  $P$ .

**Theorem 1** (Suslin's lemma [16])

Let  $\mathbf{A}$  be a commutative ring. If  $\langle v_1(X), \dots, v_n(X) \rangle = \mathbf{A}[X]$  where  $v_1$  is monic and  $n \geq 2$ , then there exist  $\gamma_1, \dots, \gamma_\ell \in E_{n-1}(\mathbf{A}[X])$  such that:

$$\langle \text{Res}(v_1, e_1 \cdot \gamma_1 {}^t(v_2, \dots, v_n)), \dots, \text{Res}(v_1, e_1 \cdot \gamma_\ell {}^t(v_2, \dots, v_n)) \rangle = \mathbf{A}.$$

Here  $e_1 \cdot x$ , where  $x$  is a column vector, stands for the first coordinate of  $x$ .

**Proof** For  $n = 2$ , let  $u_1(X), u_2(X) \in \mathbf{A}[X]$  such that  $v_1 u_1 + v_2 u_2 = 1$ . Since  $v_1$  is monic, we have  $\text{Res}(v_1, v_2 u_2) = \text{Res}(v_1, v_2) \text{Res}(v_1, u_2)$  and  $\text{Res}(v_1, v_2 u_2) = \text{Res}(v_1, v_1 u_1 + v_2 u_2) = \text{Res}(v_1, 1) = 1$ .

Suppose  $n \geq 3$ . We can without loss of generality suppose that all the  $v_i$  for  $i \geq 2$  have degrees  $< d = \deg v_1$ . For the sake of simplicity, we write  $v_i$  instead of  $\bar{v}_i$ .

Suslin's proof: It consists in solving the problem modulo an arbitrary maximal ideal  $\mathfrak{M}$  using a unique matrix  $\gamma^{\mathfrak{M}} \in E_{n-1}(\mathbf{A}/\mathfrak{M})[X]$  which transforms  ${}^t(v_2, \dots, v_n)$  into  ${}^t(g, 0, \dots, 0)$  where  $g$  is the gcd of  $v_2, \dots, v_n$  in  $(\mathbf{A}/\mathfrak{M})[X]$ . This matrix is given by a classical algorithm using elementary operations on  ${}^t(v_2, \dots, v_n)$ . One starts by choosing a minimum degree component, say  $v_2$ , then the  $v_i$ ,  $3 \leq i \leq n$ , are replaced by their remainders modulo  $v_2$ . By iterations, we obtain a column whose all components are zero except the first one. The matrix  $\gamma^{\mathfrak{M}}$  lifts as a matrix  $\gamma_{\mathfrak{M}} \in E_{n-1}(\mathbf{A}[X])$ . It follows that the first component  $w_{\mathfrak{M}}$  of  $\gamma_{\mathfrak{M}} {}^t(v_2, \dots, v_n)$  is equal to the gcd of  $v_2, \dots, v_n$  in  $(\mathbf{A}/\mathfrak{M})[X]$ . Thus,  $\text{Res}(v_1, w_{\mathfrak{M}}) \notin \mathfrak{M}$ .

A constructive proof (extracted from [18]): Let  $u_1(X), \dots, u_n(X) \in \mathbf{A}[X]$  such that  $v_1 u_1 + \dots + v_n u_n = 1$ . Set  $w = v_3 u_3 + \dots + v_n u_n$  and  $V = {}^t(v_2, \dots, v_n)$ . We suppose that  $v_1$  has degree  $d$  and for  $2 \leq i \leq n$ , the formal degree of  $v_i$  is  $d_i < d$ . This means that  $v_i$  has no coefficient of degree  $> d_i$  but one does not guarantee that  $\deg v_i = d_i$  (it is not necessary to have a zero test inside  $\mathbf{A}$ ).

We proceed by induction on  $\min_{2 \leq i \leq n} \{d_i\}$ . To simplify, we always suppose that  $d_2 = \min_{2 \leq i \leq n} \{d_i\}$ .

For  $d_2 = -1$ ,  $v_2 = 0$  and by an elementary operation, we put  $w$  in the second coordinate. We have  $\text{Res}(v_1, w) = \text{Res}(v_1, v_1 u_1 + w) = \text{Res}(v_1, 1) = 1$  and we are done.

Now, suppose that we can find the desired elementary matrices for  $d_2 = m - 1$  and let show that we can do the job for  $d_2 = m$ .

Let  $a$  be the coefficient of degree  $m$  of  $v_2$  and consider the ring  $\mathbf{B} = \mathbf{A}/\langle a \rangle$ . In  $\mathbf{B}$ , all the induction hypotheses are satisfied without changing the  $v_i$  nor the  $u_i$ . Thus, we can obtain  $\Gamma_1, \dots, \Gamma_k \in E_{n-1}(\mathbf{B}[X])$  such that

$$\langle \text{Res}(v_1, e_1 \cdot \Gamma_1 V), \dots, \text{Res}(v_1, e_1 \cdot \Gamma_k V) \rangle = \mathbf{B}.$$

It follows that, denoting by  $\Upsilon_1, \dots, \Upsilon_k$  the matrices in  $E_{n-1}(\mathbf{A}[X])$  lifting respectively  $\Gamma_1, \dots, \Gamma_k$ , we have

$$\langle \text{Res}(v_1, e_1 \cdot \Upsilon_1 V), \dots, \text{Res}(v_1, e_1 \cdot \Upsilon_k V), a \rangle = \mathbf{A}.$$

Let  $b \in \mathbf{A}$  such that

$$ab \equiv 1 \pmod{\langle \text{Res}(v_1, e_1 \cdot \Upsilon_1 V), \dots, \text{Res}(v_1, e_1 \cdot \Upsilon_k V) \rangle} = J$$

and consider the ring  $\mathbf{C} = \mathbf{A}/J$ . Note that in  $\mathbf{C}$ , we have  $ab = 1$ .

It is worth pointing out that the case where the coefficient  $a$  of degree  $m$  of  $v_2$  is a (not detected) zero simply corresponds to  $J = \mathbf{A}$ , that is, the ring  $\mathbf{C}$  being trivial (no additional computations to do).

By an elementary operation, we replace  $v_3$  by its remainder modulo  $v_2$ , say  $v'_3$ , and then we exchange  $v_2$  and  $-v'_3$ . The new column  $V'$  obtained has as first coordinate a polynomial with formal degree  $m - 1$ . The induction hypothesis applies and we obtain  $\Delta_1, \dots, \Delta_r \in E_{n-1}(\mathbf{C}[X])$  such that

$$\langle \text{Res}(v_1, e_1 \cdot \Delta_1 V'), \dots, \text{Res}(v_1, e_1 \cdot \Delta_r V') \rangle = \mathbf{C}.$$

Since  $V'$  is the image of  $V$  by a matrix in  $E_{n-1}(\mathbf{C}[X])$  (this matrix is in fact the product of two elementary matrices in  $E_2(\mathbf{C}[X])$  transforming  ${}^t(v_2, v_3)$  into  ${}^t(-v'_3, v_2)$ ), we obtain matrices  $\Lambda_1, \dots, \Lambda_r \in E_{n-1}(\mathbf{C}[X])$  such that

$$\langle \text{Res}(v_1, e_1 \cdot \Lambda_1 V), \dots, \text{Res}(v_1, e_1 \cdot \Lambda_r V) \rangle = \mathbf{C}.$$

The matrices  $\Lambda_j$  lift in  $E_{n-1}(\mathbf{A}[X])$  as, say  $\Psi_1, \dots, \Psi_r$ .

Finally, we obtain

$$\langle \text{Res}(v_1, e_1 \cdot \Psi_1 V), \dots, \text{Res}(v_1, e_1 \cdot \Psi_r V) \rangle + J = \mathbf{A},$$

the desired conclusion.  $\square$

**Remark 2** It is easy to see that in Theorem 1, with the hypothesis  $\deg v_i \leq d$  for  $1 \leq i \leq n$ , the number  $\ell$  of matrices  $\gamma_j$  in the group  $E_{n-1}(\mathbf{A}[X])$  is bounded by  $2^d$ . Moreover, each  $\gamma_j$  is the product of at most  $2d$  elementary matrices. It is worth pointing out that, in [11], there is an alternative constructive proof of this lemma using only  $\ell = d + 1$  matrices  $\gamma_j$ , each of them is the product of  $n - 2$  elementary matrices. This is substantially better than the general constructive proof we give in this paper but requires the additional condition that  $\mathbf{A}$  has at least  $d + 1$  elements  $y_1, \dots, y_{d+1}$  such that  $y_i - y_j \in \mathbf{A}^\times$  for all  $i \neq j$  (for example, if  $\mathbf{A}$  contains an infinite field). Note that we will give in Section 2 a more sophisticated and more uniform (does not depend on the  $u_i$ 's) version of that lemma in the particular case treated in [11].

**Example 3** Take  $\mathbf{A} = \mathbb{Z}$  and  $V = {}^t(v_1, v_2, v_3) = {}^t(x^2 + 2x + 2, 3, 2x^2 + 11x - 3) \in \text{Um}_3(\mathbb{Z}[x])$  (taking  $u_1 = -2x + 2$ ,  $u_2 = -3x^2 + x - 1$ ,  $u_3 = x$ , we have  $u_1 v_1 + u_2 v_2 + u_3 v_3 = 1$ ). It is worth pointing out that the  $u_i$ 's can be found by constructing a dynamical Gröbner basis for  $\langle v_1, v_2, v_3 \rangle$  [17]. Following the algorithm given in the proof of Theorem 1 and keeping the same notations, one has to perform a euclidean division of  $v_3$  by  $v_1$ , so that  ${}^t(v_1, v_2, v_3) \xrightarrow{E_{3,1}(-2)} {}^t(v_1, v_2, \tilde{v}_3 = 7x - 7)$ , and then passes to the ring  $(\mathbb{Z}/3\mathbb{Z})[x]$ . This yields to  $\ell = 2$ ,  $\gamma_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ,  $\gamma_2 = \text{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ , and finally

$$\langle \text{Res}(v_1, e_1 \cdot \gamma_1 {}^t(v_2, v_3)), \text{Res}(v_1, e_1 \cdot \gamma_2 {}^t(v_2, v_3)) \rangle = \langle 170, 9 \rangle = \mathbb{Z}.$$

This example will be pursued in the next section where as a fruit of the computations above we will obtain a free basis for the syzygy module  $\text{Syz}(v_1, v_2, v_3)$ .

## 2 Suslin's lemma for rings containing an infinite field

**Definition 4** Let  $\mathbf{A}$  be a ring containing an infinite field  $\mathbf{K}$  and let us fix a sequence  $(y_i)_{i \in \mathbb{N}}$  of pairwise distinct elements in  $\mathbf{K}$ . For instance if  $\mathbf{K} = \mathbb{Q}$  one can take  $y_i = i$ .

Let  $V = (v_1, \dots, v_n) \in \mathbf{A}[X]^n$  be an  $n$ -tuple ( $n \geq 2$ ) of polynomials such that  $v_1$  is monic with degree  $d$ . We define the resultant  $\mathcal{R}(V)$  or  $\mathcal{R}(v_1, \dots, v_n)$  of  $V$  with respect to  $X$  as the set

$$\mathcal{R}(V) := \{\text{Res}_X(v_1, v_2 + y_i v_3 + \dots + y_i^{n-2} v_n), 0 \leq i \leq (n-2)d\} \text{ if } n \geq 3, \text{ and}$$

$$\mathcal{R}(V) := \{\text{Res}_X(v_1, v_2)\} \text{ if } n = 2.$$

**Theorem 5** (Suslin's Lemma, particular case, new formulation)

Let  $\mathbf{A}$  be a commutative ring containing an infinite field  $\mathbf{K}$  and let us fix a sequence  $(y_i)_{i \in \mathbb{N}}$  of pairwise distinct elements in  $\mathbf{K}$ . Let  $v_1, \dots, v_n \in \mathbf{A}[X]$  such that  $v_1$  is monic and  $n \geq 2$ . Then

$$1 \in \langle v_1, \dots, v_n \rangle \Leftrightarrow 1 \in \langle \mathcal{R}(v_1, \dots, v_n) \rangle.$$

**Proof** The implication “ $\Leftarrow$ ” is straightforward. Let us denote by  $r_i := \text{Res}_X(v_1, v_2 + y_i v_3 + \cdots + y_i^{n-2} v_n)$ ,  $0 \leq i \leq s = (n-2)d$ , where  $d = \deg v_1$ , and suppose that  $1 \in \langle v_1, \dots, v_n \rangle$ . To prove that  $\langle r_0, \dots, r_s \rangle = \mathbf{A}$  it suffices to prove that for each maximal ideal  $\mathfrak{M}$  of  $\mathbf{A}$  there exists  $0 \leq i \leq s$  such that  $r_i \notin \mathfrak{M}$ . For this, let  $\mathfrak{M}$  be a maximal ideal of  $\mathbf{A}$  and by way of contradiction suppose that  $\overline{r_0}, \dots, \overline{r_s} = 0$  in the residue field  $\mathbf{F} := \mathbf{A}/\mathfrak{M}$ . It is worth pointing out that, denoting  $w_i = v_2 + y_i v_3 + \cdots + y_i^{n-2} v_n$ ,  $\overline{\text{Res}_X(v_1, w_i)} = \text{Res}_X(\overline{v_1}, \overline{w_i})$  since  $v_1$  is monic.

This means that for each  $i$  there exists  $\xi_i \in \overline{\mathbf{F}}$  the algebraic closure of  $\mathbf{F}$  such that  $\overline{v_1}(\xi_i) = \overline{w_i}(\xi_i) = \overline{0}$ . But since  $\deg_X v_1 = d$ ,  $\overline{v_1}$  has at most  $d$  distinct roots and hence there exists at least one root among the  $\xi_i$  repeated  $n-1$  times. We can suppose that  $\xi_0 = \xi_1 = \cdots = \xi_{n-2} := \xi$ . Thus, we have:

$$\begin{pmatrix} 1 & y_0 & \cdots & y_0^{n-2} \\ 1 & y_1 & \cdots & y_1^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & y_{n-2} & \cdots & y_{n-2}^{n-2} \end{pmatrix} \begin{pmatrix} v_2(\xi) \\ v_3(\xi) \\ \vdots \\ v_n(\xi) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since the matrix above is a Vandermonde matrix, its determinant is equal to

$$\prod_{0 \leq i < j \leq n-2} (y_j - y_i),$$

which is invertible in  $\mathbf{A}$ . Thus,  $\overline{v_1}(\xi) = \overline{v_2}(\xi) = \cdots = \overline{v_n}(\xi) = 0$ , in contradiction with the fact that  $1 \in \langle v_1, \dots, v_n \rangle$ .  $\square$

**Remark 6** Note that our Theorem 5 is a generalization of Theorem 1 of [11] since this latter corresponds to the particular case  $n = 3$ . The elementary operations performed are uniform in the sense that they do not depend on the considered unimodular vector  ${}^t(v_1, \dots, v_n)$ . As can be seen in Algorithm 2 given in the next section, this is promising for the problem of treating “globally” unimodular matrices since as mentioned in [11], treating a unimodular matrix column by column produces an explosion of the degree and gives a double-exponential complexity.

**Corollary 7** Let  $f_1, \dots, f_n \in \mathbb{Q}[X]$  ( $n \geq 2$ ) and suppose that  $f_1 \neq 0$ . Then

$$1 \in \langle f_1, \dots, f_n \rangle \Leftrightarrow \mathcal{R}(f_1, \dots, f_n) \neq \{0\}.$$

**Corollary 8** Let  $\mathbf{A}$  be a ring containing an infinite field  $\mathbf{K}$  and let us fix a sequence  $(y_i)_{i \in \mathbb{N}}$  of pairwise distinct elements in  $\mathbf{K}$ . If  $\mathcal{F} = \{f_1, \dots, f_n\} \subseteq \mathbf{A}[X]$  ( $n \geq 2$ ) is such that  $f_1$  is monic, then denoting  $\mathcal{F}' = \mathcal{R}(f_1, \dots, f_n)$ , each prime ideal of  $\mathbf{A}$  containing  $\mathcal{F}'$  is the intersection of a prime ideal of  $\mathbf{A}[X]$  containing  $\mathcal{F}$  with  $\mathbf{A}$ . In particular, we have:

$$\mathcal{F}' \subseteq \langle \mathcal{F} \rangle \cap \mathbf{A} \subseteq \sqrt{\langle \mathcal{F}' \rangle} = \sqrt{\langle \mathcal{F} \rangle} \cap \mathbf{A}.$$

**Proof** Let  $\mathfrak{p}$  be a prime ideal of  $\mathbf{A}$  containing  $\mathcal{F}'$ . Modulo  $\mathfrak{p}$ , denoting  $w_i = f_2 + y_i f_3 + \cdots + y_i^{n-2} f_n$ , we have  $\text{Res}_X(\overline{f_1}, \overline{w_i}) = \overline{0}$  for all  $0 \leq i \leq (n-2)d$ . As in the proof of Theorem 5, this means that there exists  $\xi$  in the algebraic closure of the field of fractions  $\mathbf{F}$  of  $\mathbf{A}/\mathfrak{p}$  such that  $\overline{f_1}(\xi) = \overline{f_2}(\xi) = \cdots = \overline{f_n}(\xi) = 0$ . Thus,  $\mathfrak{P} := \varphi^{-1}((X - \xi)\mathbf{F}[X] \cap (\mathbf{A}/\mathfrak{p})[X])$  is a prime ideal of  $\mathbf{A}[X]$  containing  $\mathcal{F}$  and lying over  $\mathfrak{p}$ , where  $\varphi$  is the canonical surjection from  $\mathbf{A}[X]$  to  $(\mathbf{A}/\mathfrak{p})[X]$ .

For the second part of the claim, the non trivial fact is  $\sqrt{\langle \mathcal{F} \rangle} \cap \mathbf{A} = \sqrt{\langle \mathcal{F}' \rangle}$ . For this, just write

$$\sqrt{\langle \mathcal{F} \rangle} \cap \mathbf{A} = \cap \{ \mathcal{P}, \mathcal{P} \in \text{Spec } \mathbf{A}[X] \text{ such that } \mathcal{F} \subseteq \mathcal{P} \} \cap \mathbf{A}$$

$$= \cap \{ \mathcal{P} \cap \mathbf{A}, \mathcal{P} \in \text{Spec } \mathbf{A}[X] \text{ such that } \mathcal{F} \subseteq \mathcal{P} \}$$

$$= \cap \{ \mathfrak{p}, \mathfrak{p} \in \text{Spec } \mathbf{A} \text{ such that } \mathcal{F}' \subseteq \mathfrak{p} \} = \sqrt{\langle \mathcal{F}' \rangle},$$

using the first claim. Here, for any ring  $\mathbf{B}$ ,  $\text{Spec } \mathbf{B}$  denotes the set of prime ideals of  $\mathbf{B}$ .  $\square$

### 3 Application: a new and simple algorithm for the Quillen-Suslin theorem

For any ring  $\mathbf{B}$ , when we say that a matrix  $N \in M_n(\mathbf{B})$  ( $n \geq 3$ ) is in  $SL_2(\mathbf{B})$  we mean that it is of the form

$$\begin{pmatrix} N' & 0 & \dots & 0 \\ 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

with  $N' \in SL_2(\mathbf{B})$ .

**Lemma 9 (translation by the resultant, [14] Lemma 4.2 or [16] Lemma 2.1)**

Let  $\mathbf{R}$  be a commutative ring. Let  $f_1, f_2 \in \mathbf{R}[X]$ ,  $b, d \in \mathbf{R}$ , and let  $r = \text{Res}(f_1, f_2) \in \mathbf{R}$ . Then there exists  $B \in SL_2(\mathbf{R}[X])$  such that

$$B \begin{pmatrix} f_1(b) \\ f_2(b) \end{pmatrix} = \begin{pmatrix} f_1(b+rd) \\ f_2(b+rd) \end{pmatrix}.$$

More precisely, if  $g_1, g_2 \in \mathbf{R}[X]$  are such that  $f_1 g_1 + f_2 g_2 = r$ , denoting by  $s_1, s_2, t_1, t_2$  the polynomials in  $\mathbf{R}[X, Y, Z]$  such that

$$\begin{aligned} f_1(X + YZ) &= f_1(X) + Y s_1(X, Y, Z), \\ f_2(X + YZ) &= f_2(X) + Y s_2(X, Y, Z), \\ g_1(X + YZ) &= g_1(X) + Y t_1(X, Y, Z), \\ g_2(X + YZ) &= g_2(X) + Y t_2(X, Y, Z), \end{aligned}$$

and setting

$$\begin{aligned} B_{1,1} &= 1 + s_1(b, r, d) g_1(b) + t_2(b, r, d) f_2(b), \\ B_{1,2} &= s_1(b, r, d) g_2(b) - t_2(b, r, d) f_1(b), \\ B_{2,1} &= s_2(b, r, d) g_1(b) - t_1(b, r, d) f_2(b), \\ B_{2,2} &= 1 + s_2(b, r, d) g_2(b) + t_1(b, r, d) f_1(b), \end{aligned}$$

one can take  $B = \begin{pmatrix} B_{1,1} & B_{1,2} \\ B_{2,1} & B_{2,2} \end{pmatrix}$ .

**Definition 10** We will say that a ring  $\mathbf{A}$  is equipped with a unimodularity test if given  $a_1, \dots, a_m \in \mathbf{A}$ , there is an algorithm to determine whether  $1 \in \langle a_1, \dots, a_m \rangle$  and if it is, to compute  $b_1, \dots, b_m \in \mathbf{A}$  such that  $1 = a_1 b_1 + \dots + a_m b_m$ .

Examples of rings equipped with a unimodularity test are rings having a Gröbner bases theory [3].

**Algorithm 1: an algorithm for eliminating variables from unimodular polynomial vectors with coefficients in a ring equipped with a unimodularity test and containing an infinite field**

**Input:** A column  $\mathcal{V} = \mathcal{V}(X) = {}^t(v_1(X), \dots, v_n(X)) \in \text{Um}_n(\mathbf{A}[X])$  such that  $v_1$  is monic.

**Output:** A matrix  $\mathcal{B} \in SL_n(\mathbf{A}[X])$  such that  $\mathcal{B}\mathcal{V} = \mathcal{V}(0)$ .

**Step 1:** For  $0 \leq i \leq s = (n-2)d$ , where  $d = \deg_X v_1$ , set  $w_i = v_2 + y_i v_3 + \dots + y_i^{n-2} v_n$ , compute  $r_i := \text{Res}_X(v_1, w_i)$  and find  $\alpha_0, \dots, \alpha_s \in \mathbf{A}$  such that  $\alpha_0 r_0 + \dots + \alpha_s r_s = 1$  (here we use Theorem 5 and the fact that  $\mathbf{A}$  is equipped with a unimodularity test).

For  $0 \leq i \leq s$ , compute  $f_i, g_i \in \mathbf{A}[X]$  such that  $f_i v_1 + g_i w_i = r_i$  (use Cramer's rule).

**Step 2:** Set

$$\begin{aligned}
b_{s+1} &:= 0, \\
b_s &:= \alpha_s r_s X, \\
b_{s-1} &:= b_s + \alpha_{s-1} r_{s-1} X, \\
&\vdots \\
b_0 &:= b_1 + \alpha_0 r_0 X = X \text{ (this follows from the fact that } X = \sum_{i=0}^s \alpha_i r_i X \text{)}.
\end{aligned}$$

**Step 3:** For  $1 \leq i \leq s+1$ , find  $\mathcal{B}_i \in \mathrm{SL}_n(\mathbf{A}[X])$  such that  $\mathcal{B}_i \mathcal{V}(b_{i-1}) = \mathcal{V}(b_i)$ .

In more details, let  $\gamma_i$  be the matrix corresponding to the elementary operation  $L_2 \rightarrow L_2 + \sum_{j=3}^n y_i^{j-2} L_j$ , that is,

$$\gamma_i := E_{2,n}(y_i^{n-2}) \cdots E_{2,3}(y_i).$$

For  $3 \leq j \leq n$ , set  $F_{i,j} := \frac{v_j(b_{i-1}) - v_j(b_i)}{b_{i-1} - b_i} = \frac{v_j(b_{i-1}) - v_j(b_i)}{\alpha_i r_i X} \in \mathbf{A}[X]$ , so that one obtains

$$\begin{aligned}
v_j(b_{i-1}) - v_j(b_i) &= \alpha_i r_i X F_{i,j} = \alpha_i X F_{i,j} f_i(b_{i-1}) v_1(b_{i-1}) + \alpha_i X F_{i,j} g_i(b_{i-1}) w_i(b_{i-1}) \\
&= \sigma_{i,j} v_1(b_{i-1}) + \tau_{i,j} w_i(b_{i-1}),
\end{aligned}$$

with

$$\sigma_{i,j} := \alpha_i X F_{i,j} f_i(b_{i-1}), \tau_{i,j} := \alpha_i X F_{i,j} g_i(b_{i-1}) \in \mathbf{A}[X].$$

Let  $\Gamma_i \in \mathbf{E}_n(\mathbf{A}[X])$  be the matrix corresponding to the elementary operations:  $L_j \rightarrow L_j - \sigma_{i,j} L_1 - \tau_{i,j} L_2$ ,  $3 \leq j \leq n$ , that is

$$\Gamma_i := \prod_{j=3}^n E_{j,1}(-\sigma_{i,j}) E_{j,2}(-\tau_{i,j}).$$

Set

$$B_{i,2} := \Gamma_i \gamma_i \in \mathbf{E}_n(\mathbf{A}[X]),$$

so that we have

$$B_{i,2} \mathcal{V}(b_{i-1}) = \begin{pmatrix} v_1(b_{i-1}) \\ w_i(b_{i-1}) \\ v_3(b_i) \\ \vdots \\ v_n(b_i) \end{pmatrix}.$$

Following Lemma 9, set

$$\begin{aligned}
s_{i,1}(X, Y, Z) &:= \frac{v_1(X+YZ) - v_1(X)}{Y} \in \mathbf{A}[X, Y, Z], \\
s_{i,2}(X, Y, Z) &:= \frac{w_i(X+YZ) - w_i(X)}{Y} \in \mathbf{A}[X, Y, Z], \\
t_{i,1}(X, Y, Z) &:= \frac{f_i(X+YZ) - f_i(X)}{Y} \in \mathbf{A}[X, Y, Z], \\
t_{i,2}(X, Y, Z) &:= \frac{g_i(X+YZ) - g_i(X)}{Y} \in \mathbf{A}[X, Y, Z], \\
C_{i,1,1} &:= 1 + s_{i,1}(b_{i-1}, r_i, -\alpha_i X) f_i(b_{i-1}) + t_{i,2}(b_{i-1}, r_i, -\alpha_i X) w_i(b_{i-1}) \in \mathbf{A}[X], \\
C_{i,1,2} &:= s_{i,1}(b_{i-1}, r_i, -\alpha_i X) g_i(b_{i-1}) - t_{i,2}(b_{i-1}, r_i, -\alpha_i X) v_1(b_{i-1}) \in \mathbf{A}[X], \\
C_{i,2,1} &:= s_{i,2}(b_{i-1}, r_i, -\alpha_i X) f_i(b_{i-1}) - t_{i,1}(b_{i-1}, r_i, -\alpha_i X) w_i(b_{i-1}) \in \mathbf{A}[X], \\
C_{i,2,2} &:= 1 + s_{i,2}(b_{i-1}, r_i, -\alpha_i X) g_i(b_{i-1}) + t_{i,1}(b_{i-1}, r_i, -\alpha_i X) v_1(b_{i-1}) \in \mathbf{A}[X], \\
C_i &:= \begin{pmatrix} C_{i,1,1} & C_{i,1,2} \\ C_{i,2,1} & C_{i,2,2} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{A}[X]).
\end{aligned}$$

Note that

$$C_i \begin{pmatrix} v_1(b_{i-1}) \\ w_i(b_{i-1}) \end{pmatrix} = \begin{pmatrix} v_1(b_i) \\ w_i(b_i) \end{pmatrix}.$$

Set

$$B_{i,1} := \gamma_i^{-1} \begin{pmatrix} C_i & 0 \\ 0 & I_{n-2} \end{pmatrix},$$

with

$$\gamma_i^{-1} = E_{2,3}(-y_i) \cdots E_{2,n}(-y_i^{n-2}).$$

Set

$$\mathcal{B}_i := B_{i,1} B_{i,2} \in \text{SL}_n(\mathbf{A}[X]),$$

so that  $\mathcal{B}_i \mathcal{V}(b_{i-1}) = \mathcal{V}(b_i)$ .

**Step 4:**  $\mathcal{B} := \mathcal{B}_{s+1} \cdots \mathcal{B}_1$ .

**Proposition 11** (complexity bounds, 1)

Keeping the notations of Algorithm 1, if  $\delta = \max \{\deg v_i\}$ , then the matrix  $\mathcal{B}$  is the product of at most  $(n-2)\delta + 1$  matrices in  $\text{SL}_2(\mathbf{A}[X])$  and  $4[(n-2)\delta + 1](n-2) = \mathcal{O}(n^2\delta)$  elementary matrices in  $M_n(\mathbf{A}[X])$ . Moreover,  $\deg \mathcal{B}$  is bounded by  $n\delta^{\mathcal{O}(k)}$  and the sequential complexity of this algorithm amounts to  $\mathcal{O}(n^4\delta)$  arithmetic operations in  $\mathbf{A}$  on elements of degree bounded by  $n\delta^{\mathcal{O}(k)}$ .

**Proof**

In Step 1:  $\deg w_i \leq \delta$ ,  $\deg r_i \leq \delta^2$ ,  $\deg(\alpha_i r_i) \leq \delta^{\mathcal{O}(k)}$ ,  $\deg f_i \leq \delta^{\mathcal{O}(k)}$  and  $\deg g_i \leq \delta$ .

In Step 3:  $\deg b_i \leq \delta^{\mathcal{O}(k)}$ .

In Step 4:  $\deg \mathcal{B}_i \leq \delta^{\mathcal{O}(k)}$ .

In Step 5:  $\deg G \leq n\delta^{\mathcal{O}(k)}$ .

It is immediate that  $B_{i,2} \in E_n(\mathbf{A}[X])$  is the product of  $3(n-2)$  elementary matrices in  $M_n(\mathbf{A}[X])$ , while  $B_{i,1}$  is the product of one matrix in  $\text{SL}_2(\mathbf{A}[X])$  by  $n-2$  elementary matrices. Thus,  $\mathcal{B}$  is the product of  $[(n-2)\delta + 1](4(n-2) + 1)$  matrices, among them,  $4[(n-2)\delta + 1](n-2)$  are elementary and  $(n-2)\delta + 1$  in  $\text{SL}_2(\mathbf{A}[X])$ . □

**Example 12** Now, let  $\mathcal{V} = \begin{pmatrix} x + y^2 - 1 \\ -x + y^2 - 2xy \\ x - y^3 + 2 \end{pmatrix} \in \text{Um}_3(\mathbb{Q}[x, y])$ .

Algorithm 1 has been implemented using the Computer Algebra System **Maple 8**. The code of our algorithm (**UnimodElimination**) gives a matrix  $B \in \text{SL}_3(\mathbb{Q}[x, y])$  eliminating one variable. In this example,  $B\mathcal{V} = \mathcal{V}(0, y)$ .

```
> V:=matrix([[x+y^2-1], [-x+y^2-2*x*y], [x-y^3+2]]);

> B:=UnimodElimination(V,x);

B := matrix([[1+27/151*x-56/151*x*y-24/151*x*y^2-8/151*y^3*x,
-35/151*x-4/151*x*y^2-14/151*x*y, -62/151*x-8/151*x*y^2-28/151*x*y],
[2/151*x*y+56/151*y^3*x+16/151*y^4*x+136/151*x*y^2-27/151*x,
1+84/151*x*y+8/151*y^3*x+32/151*x*y^2+35/151*x,
152/151*x*y+16/151*y^3*x+64/151*x*y^2+62/151*x],
[-56/151*x*y-8/151*y^3*x-24/151*x*y^2+27/151*x, -35/151*x-4/151*x*y^2-14/151*x*y,
1-62/151*x-8/151*x*y^2-28/151*x*y]])

> VV:=expandvector(multiply(B,V));

VV := matrix([[ -1+y^2], [y^2], [2-y^3]])
```

**Algorithm 2: an algorithm for the Quillen-Suslin theorem: case of  $\mathbf{K}[X_1, \dots, X_k]$  where  $\mathbf{K}$  is an infinite field**

Let us fix an infinite sequence of pairwise distinct elements  $(y_i)$  in  $\mathbf{K}$  and use the notation  $\underline{X} = (X_1, \dots, X_k)$ .

**Input:** One column  $\mathcal{V} = \mathcal{V}(\underline{X}) = {}^t(v_1(\underline{X}), \dots, v_n(\underline{X})) \in \text{Um}_n(\mathbf{K}[\underline{X}])$  such  $\max_{1 \leq i \leq n} \{\deg v_i\} = d$  (here by degree we mean total degree), where  $d \geq 2$ .

**Output:** A matrix  $G$  in  $\text{SL}_n(\mathbf{K}[\underline{X}])$  such that  $G\mathcal{V} = {}^t(1, 0, \dots, 0)$ .

For  $j$  from  $k$  to 1 perform steps 1 and 2:

**Step 1:** Make a linear change of variables so that  $v_1$  becomes monic at  $X_j$ .

**Step 2** Perform Algorithm 2 with  $\mathbf{A} = \mathbf{K}[X_1, \dots, X_{j-1}]$  and  $X = X_j$ . Output the new  $\mathcal{V}$ .

**Proposition 13** (complexity bounds, 2)

*Keeping the notations of Algorithm 2, we have:*

1. The matrix  $\mathcal{B}$  obtained after the first iteration (that is, after eliminating  $X_k$ ) is the product of at most  $(n-2)d+1$  matrices in  $\text{SL}_2(\mathbf{A}[X])$  and  $4[(n-2)d+1](n-2) = O(n^2d)$  elementary matrices in  $M_n(\mathbf{A}[X])$ . Moreover,

$$\deg \mathcal{B} \leq nd^{O(k)}$$

and the sequential complexity of this algorithm amounts to  $n^4d^{O(k^2)}$  field operations in  $\mathbf{K}$ .

2. The final matrix  $G$  obtained after  $k$  iterations is the product of at most  $k[(n-2)d+1]$  matrices in  $\text{SL}_2(\mathbf{A}[X])$  and  $4k[(n-2)d+1](n-2) = O(kn^2d)$  elementary matrices in  $M_n(\mathbf{A}[X])$ . Moreover,

$$\deg G \leq knd^{O(k)}$$

and the sequential complexity of this algorithm amounts to  $n^4d^{O(k^2)}$  field operations in  $\mathbf{K}$ .

**Example 14** (Example 12 continued)

$$\text{Let } \mathcal{V} = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} x + y^2 - 1 \\ -x + y^2 - 2xy \\ x - y^3 + 2 \end{pmatrix} \in \text{Um}_3(\mathbb{Q}[x, y]).$$

Recall that the syzygy module of  $(v_1, v_2, v_3)$  is

$$\text{Syz}(v_1, v_2, v_3) := \{ {}^t(w_1, w_2, w_3) \in \mathbb{Q}[x, y]^{3 \times 1} \text{ such that } w_1v_1 + w_2v_2 + w_3v_3 = 0 \}.$$

Recall also that since  ${}^t(v_1, v_2, v_3) \in \text{Um}_3(\mathbb{Q}[x, y])$ ,  $\text{Syz}(v_1, v_2, v_3)$  is a projective  $\mathbb{Q}[x, y]$ -module which is free of rank 2 by the Quillen-Suslin theorem [15, 16]. A generating set for  $\text{Syz}(v_1, v_2, v_3)$  can be obtained using Gröbner bases techniques (see for example [3, 7]). For this, let us open a **Singular** Session (for more details see [7]):

```
> ring B=0, (x,y), dp;
> ideal I=x+y2-1, -x+y2-2xy, x-y3+2;
> module N=syz(I);
> N;
```

```
N[1]=2y3*gen(1)+2xy*gen(1)+2y2*gen(3)+y2*gen(2)-y2*gen(1)+2x*gen(3)
+x*gen(2)-x*gen(1)-2*gen(3)-gen(2)-4*gen(1)
```

```
N[2]=4xy2*gen(1)-14y3*gen(1)+4xy*gen(3)+2xy*gen(2)-12xy*gen(1)
-14y2*gen(3)-7y2*gen(2)+7y2*gen(1)-10x*gen(3)-5x*gen(2)+5x*gen(1)
```

$$-2y*\text{gen}(2)+12*\text{gen}(3)+11*\text{gen}(2)+24*\text{gen}(1)$$

$$\begin{aligned} N[3]= & 8x2y*\text{gen}(1)-98y3*\text{gen}(1)+8x2*\text{gen}(3)+4x2*\text{gen}(2)-4x2*\text{gen}(1) \\ & -98xy*\text{gen}(1)-98y2*\text{gen}(3)-49y2*\text{gen}(2)+53y2*\text{gen}(1)-98x*\text{gen}(3)-53x*\text{gen}(2) \\ & +25x*\text{gen}(1)+4y*\text{gen}(3)-12y*\text{gen}(2)+8y*\text{gen}(1)+94*\text{gen}(3)+61*\text{gen}(2)+188*\text{gen}(1) \end{aligned}$$

One can read that  $\text{Syz}(v_1, v_2, v_3) = \langle u_1, u_2, u_3 \rangle$  with

$$\begin{aligned} u_1 &= {}^t(2y^3 + 2xy - y^2 - x - 4, y^2 + x - 1, 2y^2 + 2x - 2), \\ u_2 &= {}^t(4xy^2 - 14y^3 - 12xy + 7y^2 + 5x + 24, 2xy - 7y^2 - 5x - 2y + 11, 4xy - 14y^2 - 10x + 12), \\ u_3 &= {}^t(8x^2y - 98y^3 - 4x^2 - 98xy + 53y^3 + 25x + 8y + 188, 4x^2 - 49y^2 - 53x - 12y + 61, \\ & 8x^2 - 98y^2 + 4y + 94). \end{aligned}$$

But this is not a **minimal** set of generators for  $\text{Syz}(v_1, v_2, v_3)$  !

In order to obtain such a minimal generating set one has to compute a free basis for  $\text{Syz}(v_1, v_2, v_3)$ . We have implemented Algorithm 2 using the Computer Algebra System **Maple 8**. It computes a matrix  $G \in \text{SL}_3(\mathbb{Q}[x, y])$  such that  $G\mathcal{V} = {}^t(1, 0, 0)$ .

$$\begin{aligned} G := & \text{matrix}([\text{[-1+60/151*x*y^3+540/151*x*y^2+62/151*x*y-108/151*x+2*y^2-128/151*x*y^5} \\ & -272/151*x*y^4-32/151*x*y^6, \\ & -40/151*x*y^2+266/151*x*y+140/151*x-72/151*x*y^4-172/151*x*y^3+3-2*y^2-16/151*x*y^5, \\ & 248/151*x-48/151*x*y^2+484/151*x*y-144/151*x*y^4-312/151*x*y^3-32/151*x*y^5], \\ & [-y^2+64/151*x*y^5+144/151*x*y^4+2/151*x*y^3-190/151*x*y^2+27/151*x-2/151*x*y \\ & +16/151*x*y^6, \\ & 36/151*x*y^4+90/151*x*y^3+38/151*x*y^2-1-35/151*x-84/151*x*y+y^2+8/151*x*y^5, \\ & 60/151*x*y^2+72/151*x*y^4+164/151*x*y^3-152/151*x*y-62/151*x+16/151*x*y^5], \\ & [2-190/151*x*y^3-344/151*x*y^2-172/151*x*y+135/151*x-y^3+64/151*x*y^6+160/151*x*y^5 \\ & +26/151*x*y^4+16/151*x*y^7, \\ & -76/151*x*y^2-210/151*x*y-175/151*x+36/151*x*y^5+98/151*x*y^4+54/151*x*y^3-2+y^3 \\ & +8/151*x*y^6, \\ & -310/151*x-152/151*x*y^2-388/151*x*y+92/151*x*y^3+72/151*x*y^5+180/151*x*y^4 \\ & +16/151*x*y^6+1]]) \end{aligned}$$

Thus, denoting by

$$\epsilon_1 = \begin{pmatrix} -151y^2 + 64xy^5 + 144xy^4 + 2xy^3 - 190xy^2 + 27x - 2xy + 16xy^6 \\ 36xy^4 + 90xy^3 + 38xy^2 - 151 - 35x - 84xy + 151y^2 + 8xy^5 \\ 60xy^2 + 72xy^4 + 164xy^3 - 152xy - 62x + 16xy^5 \end{pmatrix},$$

and

$$\epsilon_2 = \begin{pmatrix} 302 - 190xy^3 - 344xy^2 - 172xy + 135x - 151y^3 + 64xy^6 + 160xy^5 + 26xy^4 + 16xy^7 \\ -76xy^2 - 210xy - 175x + 36xy^5 + 98xy^4 + 54xy^3 - 302 + 151y^3 + 8xy^6 \\ -310x - 152xy^2 - 388xy + 92xy^3 + 72xy^5 + 180xy^4 + 16xy^6 + 151 \end{pmatrix},$$

$(\epsilon_1, \epsilon_2)$  is a free basis for  $\text{Syz}(v_1, v_2, v_3)$ . A minimal parametrization of the set  $\mathcal{E}$  of all inverses of  $\mathcal{V}$  is

$$\mathcal{E} := \{\mathcal{U} = (u_1, u_2, u_3) \in \mathbb{Q}[x, y]^{1 \times 3} \text{ such that } \mathcal{U}\mathcal{V} = 1\} = \{\epsilon_0 + \alpha\epsilon_1 + \beta\epsilon_2, \alpha, \beta \in \mathbb{Q}[x, y]\},$$

$$\text{where } \epsilon_0 = \begin{pmatrix} -151 + 60xy^3 + 540xy^2 + 62xy - 108x + 302y^2 - 128xy^5 - 272xy^4 - 32xy^6 \\ -40xy^2 + 266xy + 140x - 72xy^4 - 172xy^3 + 453 - 302y^2 - 16xy^5 \\ 248x - 48xy^2 + 484xy - 144xy^4 - 312xy^3 - 32xy^5 \end{pmatrix}.$$

**Algorithm 3: an algorithm for eliminating variables from unimodular polynomial vectors with coefficients in a ring, general case**

**Input:** A column  $\mathcal{V} = \mathcal{V}(X) = {}^t(v_1(X), \dots, v_n(X)) \in \text{Um}_n(\mathbf{A}[X])$  such that  $v_1$  is monic.

**Output:** A matrix  $\mathcal{B} \in \text{SL}_n(\mathbf{A}[X])$  such that  $\mathcal{B}\mathcal{V} = \mathcal{V}(0)$ .

**Step 1:** Find  $\gamma_0, \dots, \gamma_s \in \text{E}_{n-1}(\mathbf{A}[X])$  such that denoting  $w_i = e_1 \cdot \gamma_i {}^t(v_2, \dots, v_n)$  and  $r_i = \text{Res}(v_1, w_i)$ , we can find  $\alpha_0, \dots, \alpha_s \in \mathbf{A}$  such that  $\alpha_0 r_0 + \dots + \alpha_s r_s = 1$  (here we use the algorithm given in the proof of Theorem 1).

For  $0 \leq i \leq s$ , compute  $f_i, g_i \in \mathbf{A}[X]$  such that  $f_i v_1 + g_i w_i = r_i$  (use Cramer's rule).

**Step 2:** Perform steps 2-4 of Algorithm 1 doing the necessary small changes.

**Example 15** (Example 3 continued)

Take  $\mathbf{A} = \mathbb{Z}$  and  $V = {}^t(x^2 + 2x + 2, 3, 2x^2 + 11x - 3) \in \text{Um}_3(\mathbb{Z}[x])$ .

A generating set for  $\text{Syz}(v_1, v_2, v_3)$  can be obtained by computing a dynamical Gröbner basis for the ideal  $\langle v_1, v_2, v_3 \rangle$  (see [1, 17]). A dynamical computation gives

$$\text{Syz}(v_1, v_2, v_3) = \left\langle \begin{pmatrix} 3 \\ -X^2 - 2X - 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -2X^2 - 11X + 3 \\ 3 \end{pmatrix}, \begin{pmatrix} -2X^3 - 11X^2 - 18X \\ 7X^3 + 14X^2 + 14X \\ X^3 + 2X^2 + 2X \end{pmatrix}, \right. \\ \left. \begin{pmatrix} -21 - 6X \\ 14 + 21X \\ 3X \end{pmatrix}, \begin{pmatrix} -4X^3 - 36X^2 - 71X + 21 \\ 14X^3 + 77X^2 - 21X \\ 2X^3 + 11X^2 - 3X + 14 \end{pmatrix} \right\rangle.$$

But of course as mentioned above this is not a minimal generating set for  $\text{Syz}(v_1, v_2, v_3)$  as it is a rank 2 free  $\mathbb{Z}[x]$ -module (by the Quillen-Suslin theorem [15, 16]). Following Algorithm 3 and doing the computations by hands (assisted by the computer algebra system **Maple 8**) we get a matrix  $G \in \text{SL}_3(\mathbb{Z}[x])$  such that

$$G V = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

```
> V:=matrix(3,1,[x^2+2*x+2,3,2*x^2+11*x-3]);

> G :=matrix([[2+29142*x^2+340*x+4788*x^3, -25686*x^2-2394*x^3-272*x-1,
-6192*x^2-2394*x^3-44*x],
[-3-43713*x^2-510*x-7182*x^3, 38529*x^2+3591*x^3+408*x+2,
9288*x^2+3591*x^3+66*x], [12+204092*x^2+2975*x+33516*x^3,
-179851*x^2-16758*x^3-2429*x-7, -43393*x^2-16758*x^3-434*x+1]]);

> det(G);

1

> F:=expandvector(multiply(G,V));
```

$$F := \text{matrix}([[1], [0], [0]])$$

Thus,

$$\left( \begin{pmatrix} -3 - 43713x^2 - 510x - 7182x^3 \\ 38529x^2 + 3591x^3 + 408x + 2 \\ 9288x^2 + 3591x^3 + 66x \end{pmatrix}, \begin{pmatrix} 12 + 204092x^2 + 2975x + 33516x^3 \\ -179851x^2 - 16758x^3 - 2429x - 7 \\ -43393x^2 - 16758x^3 - 434x + 1 \end{pmatrix} \right)$$

is a free basis for  $\text{Syz}(v_1, v_2, v_3)$ .

> inverse(G);

```
matrix([[x^2+2*x+2, 5586*x^3+14465*x^2+146*x+1, 1197*x^3+3096*x^2+22*x],
        [3, 2, 0],
        [2*x^2+11*x-3, 11172*x^3+68032*x^2+999*x+2, 2394*x^3+14571*x^2+170*x+1]])
```

The matrix  $G^{-1}$  is a completion of  $V$  into an invertible matrix as  $V$  is the first column of  $G^{-1}$ .

## References

- [1] Amidou M., Hadj Kacem A., Yengui I. *A dynamical method for computing the syzygy module over polynomial rings with coefficients in Dedekind rings*. Preprint (2007).
- [2] Caniglia L., Cortinas G., Danon S., Heintz J., Krick T., Solerno P. *Algorithmic aspects of Suslin's Proof of Serre's Conjecture*. *Comput. Complexity* **3** (1993), 31–55.
- [3] Cox D., Little J., O'Shea D. *Ideals, varieties and algorithms*, 2<sup>nd</sup> edition. New York, Springer-Verlag, 1997.
- [4] Fitchas N., Galligo A. *Nullstellensatz effectif et conjecture de Serre (Théorème de Quillen-Suslin) pour le calcul formel*. *Math. Nachr.* **149** (1990), 231–253.
- [5] Fabianska A., Quadrat A. *Applications of the Quillen-Suslin theorem to multidimensional systems theory*. INRIA Report 6126 (2007).
- [6] Fliess M., Mounier H. *Controllability and observability of linear delay systems: an algebraic approach*. *ESAIM: Coccv.* **3** (1998), 301–314.
- [7] Greuel G.M., Pfister G. *A Singular introduction to commutative algebra*. Springer Verlag Berlin, Heidelberg, New York, 2002.
- [8] Lim Z. *On syzygy modules for polynomial matrices*. *Linear Algebra Appl.* **298** (1999), 73–86.
- [9] Lim Z., Bose N. K. *A generalization of Serre's conjecture and related issues*. *Linear Algebra Appl.* **338** (2001), 125–138.
- [10] Logar A., Sturmfels B. *Algorithms for the Quillen-Suslin theorem*. *J. Algebra* **145** no. 1, (1992), 231–239.
- [11] Lombardi H., Yengui I. *Suslin's algorithms for reduction of unimodular rows*. *J. Symb. Comp.* **39** (2005), 707–717.
- [12] Park H. *Symbolic computations and signal processing*. *J. Symb. Comp.* **37** (2004), 209–226.
- [13] Park H., Kalker T., Vetterli M. *Gröbner bases and multidimensional FIR multirate systems*. *Journal of Multidimensional systems and signal processing* **8** (1997), 11–30.
- [14] Park H., Woodburn C. *An algorithmic proof of Suslin's stability theorem for polynomial rings*. *J. Algebra* **178** (1995), 277–298.
- [15] Quillen D. *Projective modules over polynomial rings*. *Invent. Math.* **36** (1976), 167–171.
- [16] Suslin A. *On the structure of the special linear group over polynomial rings*. *Math. USSR-Izv.* **11** (1977), 221–238.

- [17] Yengui I. *Dynamical Gröbner bases*. J. Algebra **301** (2006), 447–458.
- [18] Yengui I. *Making the use of maximal ideals constructive*. Theoret. Comput. Sci., to appear.
- [19] Youla D.C., Pickel P.F. *The Quillen-Suslin Theorem and the structure of  $n$ -dimensional elementary polynomial matrices*. IEEE Trans. Circuits Syst. **31** (1984), 513-517.